

• HOW WE WORK

You own your infrastructure. We operate it.

Linux and Kubernetes operations built on open source, with no lock-in.

KubeAid

Your complete, digitally sovereign work platform

Productivity, collaboration, communication and AI – all in one sovereign platform.



Digitally sovereign

Your data. Your infrastructure. Your rules.

- ✓ No vendor lock-in
- ✓ Data stays in your control
- ✓ Compliant with European regulations



Sovereign infrastructure

Hosted in your region (or your own environment)



End-to-end security

Encrypted, auditable, compliant



Open standards

Interoperable and flexible



Sustainable

Efficient use of resources



Built for teams

From small teams to large organisations



LinuxAid

Powering your Linux systems

A dedicated platform for developers and engineers using Linux.



For developers & engineers

- ✓ Linux distributions
- ✓ Developer tools
- ✓ System administration
- ✓ Secure and sovereign

Some of the teams we have worked with

GN

KILROY

TDC Group

HBK
HOTTINGER BRÜEL & KJÆR

youSee

ebillet

**BERLINGSKE
MEDIA**

churchdesk

**BLACK
WOOD
SE7EN**
™

T E L M O R E

Officient

NAVIPARTNER

"I am incredibly happy partnering with Obmondo for our operations and we have worked with them for 10+ years."

Esben Madsen
CEO, Ebillet a/s

"Obmondo has been our technology partner for everything open source. Their open-source automation frameworks and customized solutions ensure uptime for GN."

Jakob Ovesen
Linux Architect, GN Store Nord

"Information like servers running Red Hat and other stuff was extremely hard to get before we started working with Obmondo. Obmondo also streamlined security updates and maintenance, making things much easier for the team."

Mark Gittins
Senior DevOps Engineer, HBK

The story in eleven chapters

00

Our open-source approach

Why KubeAid and LinuxAid are public

01

Digital sovereignty

You own it, we operate it

02

How we work

Part of your team

03

Services

What we take over

04

Onboarding

Access comes first

05

Security and access

Hardware keys, zero trust

06

Monitoring and alerts

Security, alerts and deadlines

07

Backup strategy

Set by your recovery goals

08

Restore and disaster recovery

Tested, not assumed

09

Pricing and contract

Per server, month to month

10

SKI 02.22

Hybrid operations

Our founder's 25 years of Linux operations, published as open source

Our founder has worked in Linux operations for more than 25 years. We put that experience into two open-source projects, KubeAid and LinuxAid.

They set up servers and clusters from Git and cover what every production system needs: security, updates, backup and recovery.

The code is shared. A fix or feature we build for one customer reaches every customer running the same project, which lowers the cost of a secure setup for all of them.

IN KUBE Aid TODAY

120+

Helm charts in the public KubeAid repository, shared by every customer who runs KubeAid.



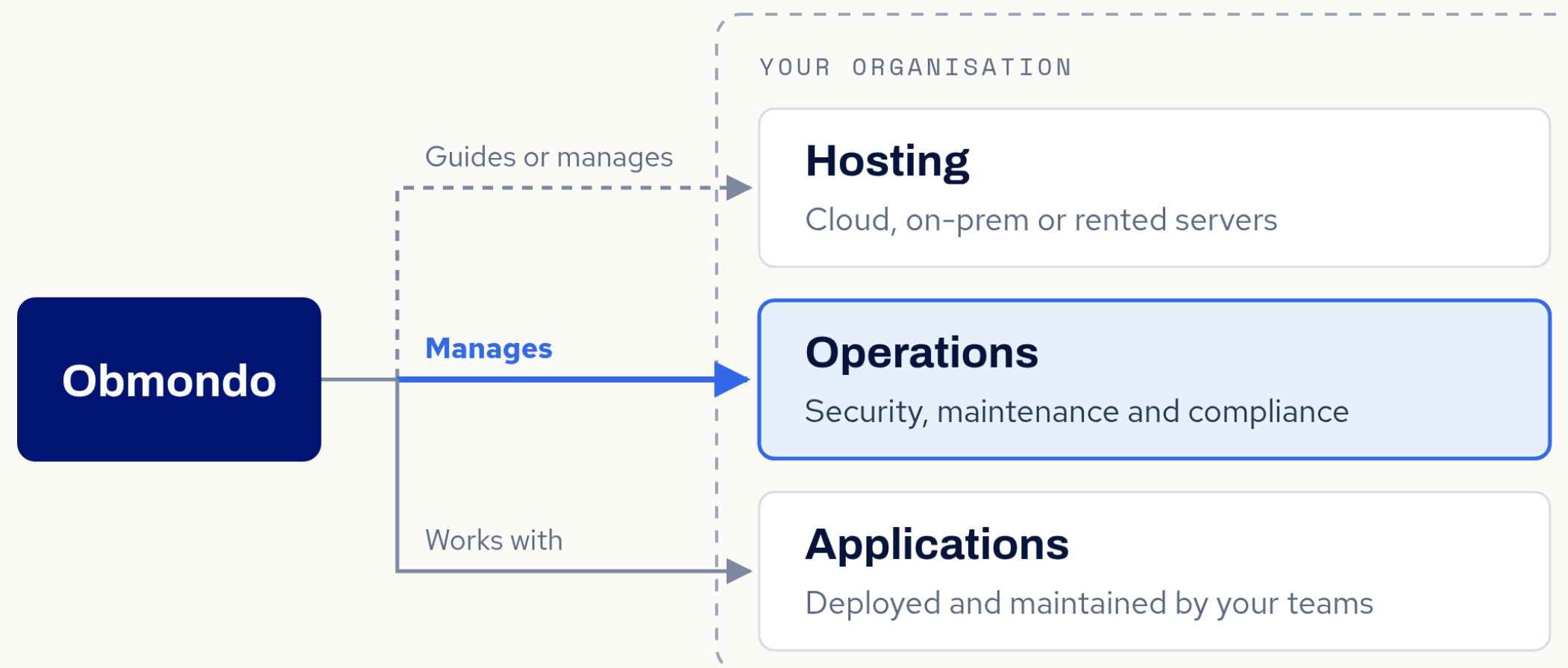
For Kubernetes
kubaid.io



For Linux servers
linuxaid.io

Your hosting, your accounts, your root access

Wherever your systems run, the environment stays yours.



YOU KEEP CONTROL OF

- ✓ The hosting provider
- ✓ The servers and cloud accounts
- ✓ Application code and architecture
- ✓ Root access and admin rights

We run the operating-system layer: hardening, patching, compliance, monitoring, backups and recovery planning. If you want us to, we can also handle hardware and network issues with your hosting provider.

Leave at any time, at near-zero cost

Many managed service providers make switching expensive with proprietary tooling, custom monitoring stacks and platform-specific configuration. We build on open source instead, and you own everything, so it just keeps running if you leave.

01

Month to month

Billed by the month, with no long-term commitment. You change or cancel your plan yourself in the portal, and support ends with the current period.

02

Your configuration, your Git

Your configuration lives in its own Git repository. You can host it yourself on GitHub, GitLab, Gitea and others, and give us a deploy key you can revoke.

03

Anyone can take over

Monitoring, alerting and backups are documented and reproducible, on open-source tooling. Another provider can take over without a rebuild.

If we stop delivering the quality you expect, you can replace us straight away.

Service levels on response time, not on uptime you control

A classic uptime SLA assumes one vendor controls the whole stack. You control yours, so we don't promise what only you control.

OUTSIDE OUR CONTROL

- ✗ Your network's reliability
- ✗ Your hosting provider's uptime
- ✗ Changes your own teams make on servers you control

WHAT WE COMMIT TO

- ✓ Response times from your support plan, from 1 business day down to 1 hour, 24×7
- ✓ Vulnerability/CVE monitoring and patching
- ✓ Operations and developer support

It's a deliberate trade-off. You keep control, and nothing ties you to us.

Part of your Dev and Ops teams

EXISTING SYSTEMS

We work with what you run

We use the systems, tools and infrastructure you already have, and improve them with you.

NEW SYSTEMS

We build it from scratch

We build a new environment on LinuxAid or KubeAid, following industry best practice, and move your services onto it.

Watch

Monitoring goes in first and keeps running.

Review

We look at your environment's strengths and weak spots.

Improve

We propose concrete improvements and plan them with you.

Share

Unless agreed otherwise, the work goes into LinuxAid or KubeAid for every customer.

Shared improvements, shared cost

Many customers run the same open-source projects. When work improves a project, the customers who benefit split the cost.

EXAMPLE · ONE TASK · 30 HOURS OF DEVELOPMENT AND TESTING



5 hours

Your share, on your invoice

25 hours

Paid by the other customers who get the same improvement

In the customer portal, shared work is a feature that customers sponsor. Its cost is split equally or by each customer's number of nodes, and every approved hour appears as a comment on its ticket.

What we take over, what stays yours

Linux and Kubernetes setup

New servers and clusters on LinuxAid and KubeAid, with your services moved onto a clean, standard base. Or we start by adding monitoring to what you run today.

Monitoring

On plans with a response time, from Bronze up, alerts go straight to our operations team. We host the monitoring by default, or you run your own Prometheus and Puppet and forward alerts to us.

Backups and restores

We set up and run backup and restore for your infrastructure, matched to your reliability requirements.

Upgrades and security updates

OS and application security updates, beyond what the base distribution ships, rolled out in service windows you choose. We manage the package repositories end to end, ideally from a dedicated repository server.

STAYS WITH YOU UNLESS AGREED

- Custom application deployments
- Business-specific configuration
- Access management
- Internal approval workflows

The customer portal lists each server's open CVEs and its next update window.

Access first, then a full assessment

1 Access

Bastion or VPN access comes first. The timing depends on how fast your firewall rules and routing are ready.

2 Onboard

Add a server in the customer portal at obmondo.com and run the install command it gives you, as root. Or give us SSH/VPN access and we do it.

3 Assess

We review configuration, security and access, backup and recovery, monitoring, operational health and architecture.

4 Roadmap

Together we agree on an improvement roadmap and a long-term operating plan.

Existing Kubernetes clusters

We can monitor an existing cluster for a short period while we design a new KubeAid cluster that fixes the issues we find.

Already running Puppet?

We recommend LinuxAid's Puppet setup, built on OpenVox, the community fork of Puppet. Its agent replaces the puppet-agent package, and it can run entirely on your own hosts.

Zero trust, on hardware keys

Every engineer's identity lives on a YubiKey. The private key can't be read off it, a PIN unlocks it, and every operation needs a physical touch. Access can't be shared, phished or used silently by a compromised machine.

Touch

for every login, signature and decryption

1 identity

SSH and GnuPG, per engineer

THREE WAYS IN

- **Outgoing bastion.** A small VM in your network opens an SSH-only tunnel out to us.
- **Incoming bastion.** Port 22, reachable only from our fixed IPs in Denmark, Germany and Finland.
- **NetBird VPN.** Open-source WireGuard VPN with Keycloak login and MFA.

LOGINS, SECRETS AND AUDIT

- On KubeAid clusters, Kubernetes access runs over NetBird, with the Keycloak sign-in mapped to Kubernetes roles.
- Passwords live in pass, from passwordstore.org, and every secret needs its own touch.
- Audit logs show who accessed a cluster, when, as whom, and which Kubernetes actions they ran.

You can read every rule we alert on

Your servers and clusters are monitored by Prometheus with our open-source alert rules, published at github.com/Obmondo/KubeAid.

Servers, with LinuxAid

- Host and hardware metrics
- CPU, RAM, I/O and disk health
- Filesystems and storage
- Network performance

The rules are updated regularly and covered by their own test suite.

Kubernetes, with KubeAid

- Nodes, pods and containers
- etcd performance
- Ingress, services and network
- Control plane and API server
- Scheduler and controller-manager
- Selected open-source apps

Built on kube-prometheus, with our own rules on top and optional alert packs per cluster.

If you want, we leave specific hosts or components out of alerting.

Security monitoring and mitigation

linuxaid | SERVERS

- **Known vulnerabilities.** The portal lists each server's open CVEs, with severity and the next update window.
- **End of life.** An alert 75 days before the OS release stops getting free security updates, and again once it has.
- **Firewall.** An alert when the firewall starts blocking an unusual amount of traffic, a sign of breach attempts.
- **Hardening.** SSH only allows strong key exchange, ciphers and MACs, and auditd and SELinux can be switched on per server.
- **Repo snapshots.** Packages come from a dated snapshot, moved forward the day before each update cycle, so every server gets the same updates.

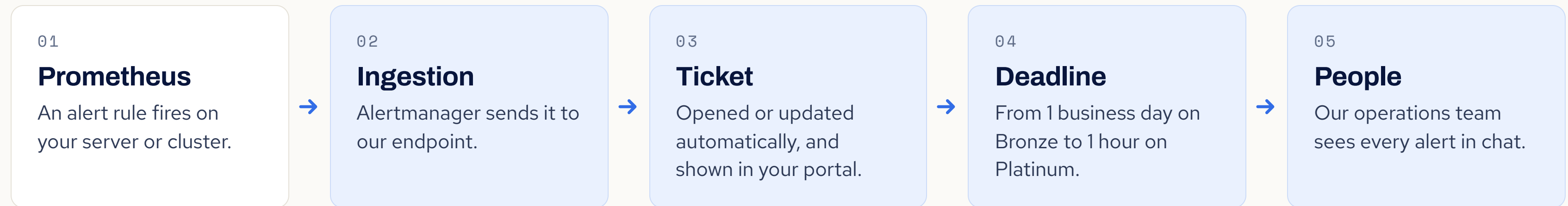
kubeaid | KUBERNETES

- **Supply chain security.**
 - **Image scanning.** Trivy scans the container images you run for known vulnerabilities, and the portal shows the results.
 - **Registry mirror.** Harbor can mirror those images and scan them too.
- **End of life.** An alert when the cluster's Kubernetes version gets close to end of life.
- **Firewall.** Cilium network policies filter ingress and egress traffic, and an alert fires when denied traffic stays high, a sign of breach attempts.
- **Runtime security.** Tetragon watches process and network activity in the cluster, and KubeArmor can block what your policies forbid.
- **Admission policies.** Kyverno or Gatekeeper can stop workloads that break your rules before they start.

Image scanning, runtime detection and admission policies are options you switch on per cluster.

Fixes roll out in the service windows you choose, as pull requests in your own config repository.

With Bronze or higher, every alert becomes a ticket with a deadline



ESCALATION

The on-call engineer is alerted when a response deadline is less than an hour away. Critical alerts also go to management.

Alerts that fire during your service window are held back. If they are still firing when the window ends, they become tickets.

Most alerts fire before any services are affected, giving us time to fix the problem before anything breaks. When something does break, we restore service first, then fix the root cause.

Backups set by your recovery goals

Your RPO is how much data you can afford to lose. Your RTO is how fast you need it back. We start from what already works for you and recommend changes where it falls short.

WHERE WE START

- **New installations.** Give us a blank server, usually a minimal Ubuntu or Debian LTS, and we deliver a fully open-source backup setup.
- **Existing systems.** We assume nothing about what's configured, and we agree a path with you before changing anything.

METHODS

- **Point-in-time recovery** for PostgreSQL, with WAL archived to S3, and for other systems that support it.
- **Kubernetes storage snapshots** for fast local recovery, pushed to S3 for host redundancy.
- **Offsite copies.** We recommend replicating the backup server to a second location.

STORAGE AND ENCRYPTION

- S3-compatible storage.
- Client-side encryption, which we recommend, or LUKS on the backup server's data disk.
- Always encrypted in transit, over HTTPS or SSH.

Restores are tested, not assumed

RECOVERY TESTS

Planned with you, logged on a ticket

ISO 27001 and NIS2 typically require regular recovery tests. Every hour spent on one is posted on its ticket, like all our work.

- ✓ **Reproducible clusters.** The KubeAid CLI builds every KubeAid cluster the same automated way. Rebuilds need fewer manual steps, and there is less data to back up.
- ✓ **What drives restore time.** A full restore depends on storage size, cloud or on-prem, and which snapshots and WAL are available.
- ✓ **Shared lessons.** A fix found in one customer's test reaches every customer on LinuxAid and KubeAid.

Priced per server, month to month

PLAN	SERVICE LEVEL
● Basic	Monitoring and live chat
● Bronze	Response within 1 business day
● Silver	4-hour response in business hours
● Gold	2-hour response, 24×7
● Platinum	1-hour response, 24×7

- ✓ Volume discounts apply automatically as you add servers.
- ✓ Advice and operations work is billed as consultation, per minute. The calculator shows the free consultation hours for your plan mix.
- ✓ Business hours are 08:00 to 17:00 in your primary time zone, on business days.
- ✓ Cancel whenever you want. Support ends with the current subscription period.

Current prices and the calculator:
obmondo.com/pricing

How we fit into SKI 02.22

SKI 02.22 covers IT operations of any scope, from full outsourcing to hybrid setups where organisations keep their infrastructure and outsource specific parts to specialised suppliers.

We fit the hybrid model. We run the operations layer: security updates, monitoring, backup strategy and day-to-day infrastructure operations. Hosting and applications stay with you.

Operations layer only, by design. You keep control of your infrastructure, data location, security posture and vendor choices.

Applications

YOU OR YOUR VENDOR

Operations

Security updates, monitoring, backups,
daily operations

OBTMONDO

Hosting

YOU AND YOUR PROVIDER



• NEXT STEP

Talk to us about your setup

[Book a meeting](#)

EMAIL AND PHONE

sales@obmondo.com · +45 61 28 12 00

WEB

obmondo.com

OPEN SOURCE

github.com/Obmondo · kubead.io · linuxaid.io